

國立臺東女子高級中學/機關

109年度資通安全維護計畫實施情形線上審查意見改善報告

說明：

1. 依據資通安全法第十二條規定公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。
2. 依據資通安全法第十三條規定公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。

題號	評量項目	審查意見	改善情形
1.3	組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	應提供資通安全政策審核紀錄及公告紀錄	提供本校資通安全工作小組會議紀錄及校務會議需宣導資通安全紀錄。
1.4	組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	佐證資料不符，應提供管審會紀錄	提供本校資通安全工作小組會議紀錄
3.3	是否具備相關專業資安證照或認證？	應提供專業安證照及職能訓練證明	檢附本校資安研習紀錄
5.1	人員進入重要實體區域是否訂有安全控制措施？	應提供機房門口管制措施，如門禁刷卡或鑰匙開啟	D-019 人員進出機房登記表，並於4月完成改善機房門禁及監視系統，並提供進出門禁管制表。
5.2	重要實體區域的進出權利是否定期審查並更新？	未提供佐證資料	提供 D-019 人員進出機房登記表。
5.3	電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	未提供佐證資料	提供 D-019 人員進出機房登記表，並於4月完成改善機房門禁及監視系統，並提供進出門禁管制表。
5.5	各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	佐證資料不符，應提供消防、CCTV、門禁設施檢查紀錄或保養資料。設備使用訓練紀錄	提供各項安全設備定期檢查紀錄，及設備安全使用教育訓練紀錄。
5.6	第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	佐證資料不符，應提供未具機房進出權限之人員，進出機房應有授權	提供具機房進出權限之人員，進出機房應有授權人員陪同之照片。

題號	評量項目	審查意見	改善情形
		人員陪同之照片	
5.7	重要資訊處理設施是否有特別保護機制？	佐證資料不符，應提供實體安全管理制度文件	提供 D-025 備份狀況紀錄表、不斷電系統設備與運作佐證資料。
5.10	通訊線路及電纜線是否作安全保護措施？	佐證資料不符，應提供線路保護設施照片	提供通訊線路及電纜線安全保護措施佐證照片
5.11	設備是否定期維護，以確保其可用性及完整性？	未提供佐證資料	提供設備定期維護紀錄
5.12	設備送場外維修，對於儲存資訊是否訂有安全保護措施？	未提供佐證資料	提供 D-021 設備進出紀錄表
5.14	設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	未提供佐證資料	提供 D-010 資訊資產異動申請表
5.20	是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	未提供佐證資料	提供網頁公告及校務會議宣導資料
5.21	重要的資料及軟體是否定期作備份處理？	未提供佐證資料	提供 D-025 備份狀況紀錄表
5.22	備份資料是否定期回復測試，以確保備份資料之有效性？	未提供佐證資料	提供 D-025 備份狀況紀錄表
5.23	對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	未提供佐證資料	提供系統登作畫面、https、檔案加密。
5.24	是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	未提供佐證資料	提供 C-005 可攜式設備及儲存媒體使用與管理作業要點
5.25	是否訂定使用者存取權限註冊及註銷之作業程序？	未提供佐證資料	提供 D-028 帳號清查紀錄表、D-029 帳號清查結果報告。
5.26	使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	未提供佐證資料	提供 D-028 帳號清查紀錄表、D-029 帳號清查結果報告。
5.31	是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	未提供佐證資料	提供 C-005 可攜式設備及儲存媒體使用與管理作業要點。

題號	評量項目	審查意見	改善情形
5.33	系統變更後其相關控管措施與程序是否檢查仍然有效？	未提供佐證資料	提供資訊服務變更管理制度及紀錄。
5.34	是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	未提供佐證資料	提供網頁系統弱點掃描報告
5.35	限制使用危害國家資通安全產品	佐證資料不符，應提供使用大陸品牌資訊產品清單，或說明未使用大陸品牌資訊產品	提供清查本校各處室未使用大陸品牌資訊產品證明。
6.2	機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	應提供宣導及公告相關資料	提供網頁公告及校務會議宣導資料
7.1	是否定期辦理資通安全認知宣導？	佐證資料不符，應提供資通安全公告、宣導及研習資料，非資安通報平台畫面	提供本校資通安全公告、宣導及研習資料
7.2	是否對同仁進行資安評量？	應提供人員資安評量或資安研習評量資料	於6月進行本校同仁資安研習並進行資安研習評量。
8.1	是否設有稽核機制？	未提供佐證資料	提供 B-013 資訊安全稽核作業程序書。
8.2	是否定有年度稽核計畫？	未提供佐證資料	提供 B-013 資訊安全稽核作業程序書。預計6月份進行內部稽核。
8.3	是否定期執行稽核？	未提供佐證資料	提供 B-013 資訊安全稽核作業程序書。預計6月份進行內部稽核。
8.4	是否改正稽核之缺失？	未提供佐證資料	提供 B-013 資訊安全稽核作業程序書。預計6月份進行內部稽核。
9.1	是否訂定安全維護計畫持續改善機制？	未提供佐證資料	提供本校資通安全會議資料
9.2	是否追蹤過去缺失之改善情形？	未提供佐證資料	提供本校資通安全會議資料
9.3	是否定期召開持續改善之管理審查會議？	未提供佐證資料	提供本校資通安全會議資料
10.1	資通系統委外(含委辦)是否簽訂協議書或契約？	未提供佐證資料	提供委外契約書及 D-022 委外廠商保密切結書。
10.2	是否落實檢核及履約督導管	未提供佐證資料	110 年開始分年度進行不同

題號	評量項目	審查意見	改善情形
	理？		部分重點項目健檢。
10.3	委外(含委辦)相關人員是否簽訂保密合約書？	未提供佐證資料	提供委外契約書及 D-022 委外廠商保密切結書。
11.2	是否配置一名資通安全專責人員？	未提供佐證資料	提供 D-001 資訊通安全組織成員表。
11.3	是否每兩年辦理一次資通安全健診？	未提供佐證資料	110 年開始分年度進行不同部分重點項目健檢。

承辦人/專責人員

教師兼圖書館主任 鄭華鈞

單位主管

教師兼圖書館主任 鄭華鈞

校長

國立臺東女子高級中學 校長 王琨